Best Practices for Cyber Risk Management Success

Maturity Models are a popular technique that organizations use to evaluate certain business processes to produce a desired set of outcomes. They map an actionable path towards a more organized and systematic way of doing business. When it comes to third-party vendor risk management in healthcare, maturity models can help healthcare delivery organizations (HDOs) understand where they are – and where they want to be – in terms of the people, processes, and technologies deployed.

This report presents a proven maturity model to successfully transform a third party risk management program. Learn the best practices, milestones, and outcomes across each maturity level to develop a more sophisticated, robust third party risk management program and accelerate time-to-value from resource investments:

Level 0 - Initial State

At the start of their third party risk management journey, many HDOs find themselves struggling to scale their program; and, despite heroic efforts, resource-constrained teams face myriad challenges, including:

- Existing risk management processes are ad-hoc and manual, with little-to-no meaningful automation deployed.
- There is no central repository for vendor risk data and evidence. Vendor data is manually shared, analyzed and stored using legacy tools such spreadsheets, emails, and other unstructured applications.
- Communication between departments is siloed, and, as a result, risk processes are often poorly defined and inconsistent across the organization.
- Most vendor risk assessments are outdated with only perceived "high-risk" vendors regularly assessed at procurement.
- Risk assessors must juggle a different set of questions for each vendor, while risk scoring and summary reporting is often ad-hoc and non-standardized.
- General awareness of cyber risk exists, but an organization-wide policy has not been implemented; moreover, best practices for enterprise risk like NIST Cybersecurity Framework (NIST CSF) are poorly documented and/or not yet adopted.

Maturity Level 1 - Implemented

At this maturity level, a vendor risk management (VRM) system may be in the early stages of implementation and teams are learning to coordinate and centralize their third party risk management program. Milestones include:

- A VRM system is selected and in early stages of deployment.
- A small number of risk assessors are beginning to use the platform, while concurrently running prior processes as confidence builds in the new system.
- Process workflows are standardized and mapped to the VRM system to begin driving efficiencies and scale
- Vendors and associated products are mapped to the VRM system along with historical assessment data, building a centralized view to drive risk management program strategy

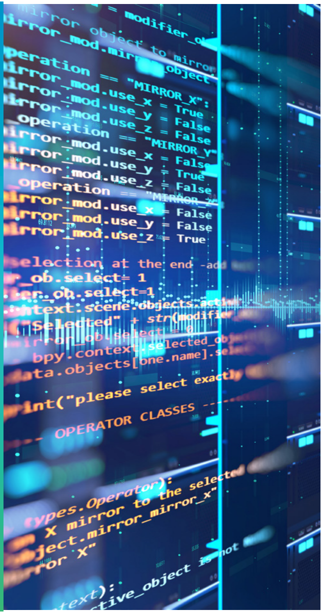
Outcomes: At this maturity level, organizations are focusing on standardizing their processes around a centralized VRM platform and beginning to manage risk as a holistic, ongoing practice. As workflows and processes become more automated, resources are able to be re-deployed to focus on overall risk management program strategy.

Maturity Level 2 - Adopted

At the next level of maturity, teams are building confidence around their use of the centralized platform and automated workflows. Risk data is now exchanged (on a limited basis) across departments and assessment completion times are now measurable. What's more, vendor risk management processes are better defined and documented, cybersecurity policies begin to be documented, and the coordination of risk governance begins.

Outcomes: Best performers at this maturity level are able to leverage the centralized platform to inform their current processes and guide accretive changes to their workflows – ensuring repeatable and consistent outcomes. A minimum of 50% of new assessments are performed through the VRM system.

> *"Censinet RiskOps enables us to automate and streamline our IT cybersecurity, third-party vendor, and supply chain risk programs in one place. Censinet enables our remote teams to quickly and efficiently coordinate IT risk operations across our health system."*
>
> — Aaron Miri, Senior Vice President, Chief Digital & Information Officer, Baptist Health



Maturity Level 3 - Standardized

At Level 3 maturity, organizations are proactive about third party risk management and are using automated, coordinated processes. Standardized and unified processes are identified and defined for enterprise risk management across multiple departments, including IT, Information Security, Supply Chain, Compliance, and Legal. Key milestones include:

- New vendors are tiered based on risk and potential impact to the business and reassessments are automatically scheduled for all new vendor assessments.
- Risk is managed across the full contract lifecycle for all vendors and products – from evaluation to procurement, implementation to usage, renewal to retirement.
- Integrations are configured between the VRM system and workflow ticketing systems (e.g., ServiceNow) to centralize and coordinate risk management and innovation adoption across the enterprise.
- Automation is used to streamline all third party risk workflows and optimize resources; what's more, risk assessment completion times are continuously measured, tracked, and begin to significantly decrease over time as automation gains are realized.
- Risk governance is coordinated across internal and external organizations.
- Regular risk scoring, reporting, and risk visibility is shared with executive leadership

Outcomes: By Level 3 maturity, meaningful automation gains from a centralized VRM system are realized, with all new assessments managed in the platform and over 50% of historical assessments migrated to the VRM system and managed across the lifecycle going forward.

Maturity Level 4 - Integrated

Cybersecurity, operational, and enterprise risk are integrated across all business processes at this maturity level. Executive leadership and the Board of Directors are fully engaged with cyber risk management, requiring regular updates on third party and enterprise risk management activity, risk scores, best practice coverage, and security program performance and maturity. Other significant milestones include:

- Reassessment frequency is scheduled according to the risk tier for each vendor and product (i.e., Critical and High Risk products are reassessed annually).
- Automated corrective action plans and remediations are generated and tracked for all third parties, including: vendors, products, medical devices, BioMed, IRB/research, non-technical suppliers, internally developed applications, and affiliated facilities.
- Annual participation in benchmarking surveys is used to compare cybersecurity performance to peers; in addition, organizations perform regular self-assessments of coverage for HHS Health Industry Cybersecurity Practices (HICP) and NIST CSF.

Outcomes: 100% of risk assessments and reassessments are managed in the VRM platform with automated corrective actions and remediations tracked, mitigated and/or closed to reduce third party risk. Continuous improvement in enterprise risk is realized through peer benchmarking and self-assessment of recognized security practices (HICP and NIST CSF).

Maturity Level 5 - Transformed

At the final maturity level, all risk management objectives and activities are aligned with the overall strategic goals of the organization. For third party risk, 100% of risk assessments and reassessments, corrective actions and remediations, and risk scoring and summary reporting are managed through the VRM platform by all stakeholders across the organization. Cyber risk data is shared between all industry participants across a secure, frictionless risk exchange in a collaborative effort to strengthen risk posture and cybersecurity for all.

Enterprise risk management is fully automated and continuously monitored and updated based on regulatory changes, changes in business requirements and technology, and an ever-evolving threat landscape. What's more, enterprise risk management systems adapt and respond in real-time using threat intelligence, network sourcing, peer benchmarking, and predictive indicators.

Final Thoughts

The Censinet RiskOps™ Maturity Model described above maximizes return on investment and accelerates time-to-value for an HDO's third party and enterprise risk program. An American Hospital Association (AHA) Cybersecurity Preferred Solution Provider, Censinet is the first and only purpose-built risk exchange for managing cyber risk in healthcare. If you would like to learn more, contact us at info@censinet.com or visit censinet.com.

> *"Every individual, department and business unit within your organization that purchases technology, services and supplies should be educated about your organizational cybersecurity requirements for third parties and the potential cybersecurity risks to the organization that is involved in work using third-party vendors."*
>
> — John Riggi, National Advisor for Cybersecurity and Risk, American Hospital Association

KLAS RESEARCH
CENSINET®
MEASURED
Cybersecurity Transparent

American Hospital Association™
Preferred Cybersecurity Service

CHIME®

Censinet is an American Hospital Association Preferred Cybersecurity Service Provider for Cyber Firm Risk Management and Information Governance and Cyber Risk Assessment, Privacy and HIPAA Compliance.